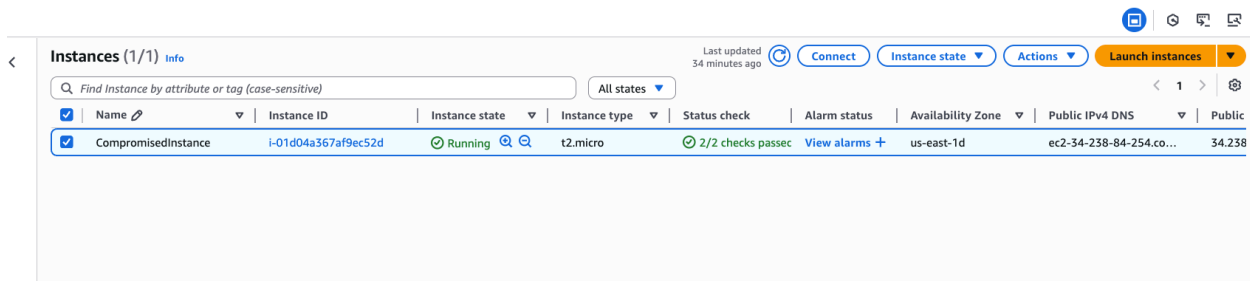


Threat Detection and Containment: A malicious actor compromises an EC2 instance and initiates unauthorized data exfiltration.

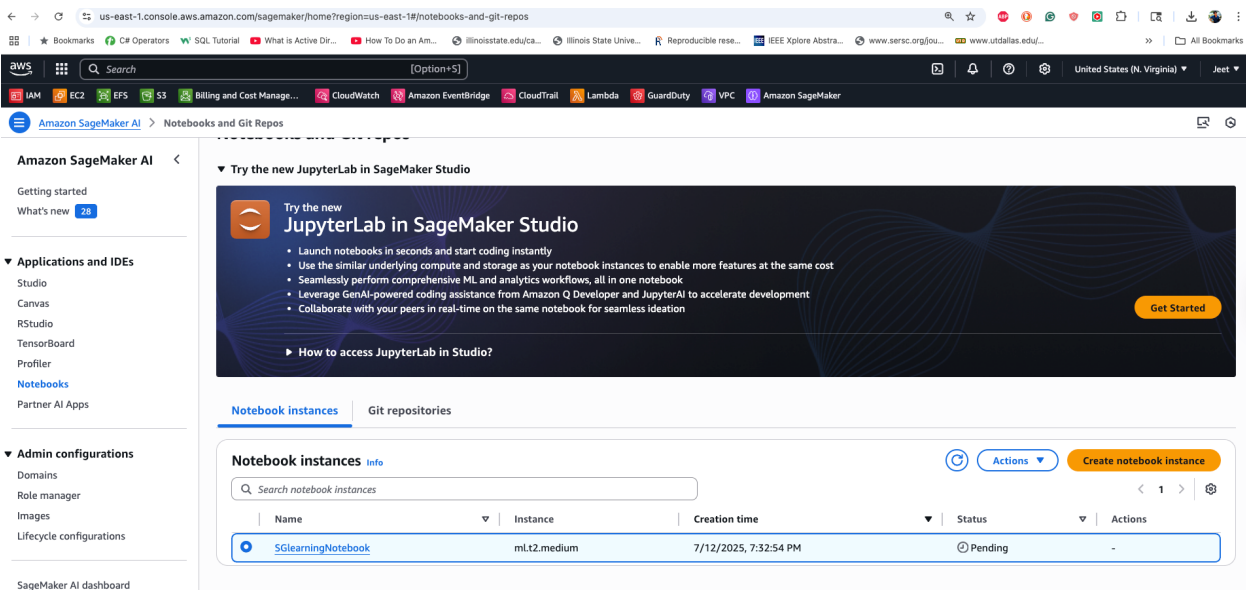
1. Detection: Amazon VPC Flow Logs reveal abnormal outbound traffic. A SageMaker machine learning model identifies this behavior as anomalous



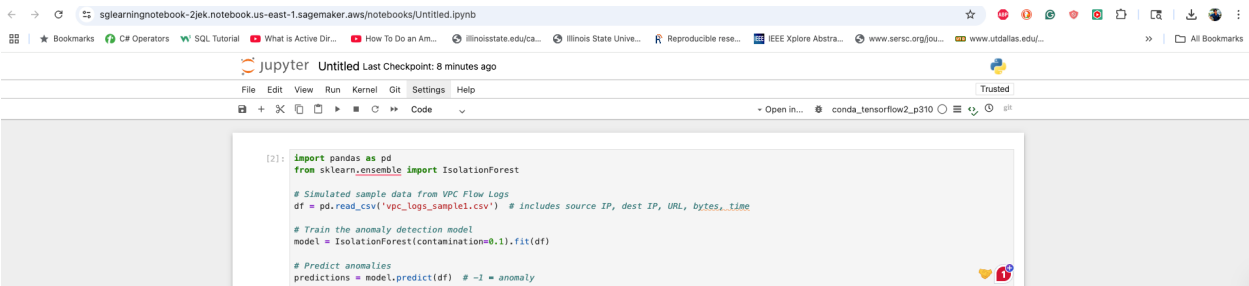
	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public
<input checked="" type="checkbox"/>	CompromisedInstance	i-01d04a367af9ec52d	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1d	ec2-34-238-84-254.co...	34.238

```
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
ec2-user@ip-172-31-86-66 ~]$ curl -i https://www.facebook.com/
HTTP/2 200
vary: Accept-Encoding
set-cookie: fr=0LYxwUjXRRYof1CyW..BocvXX..AAA.0.0.BocvXX.AWfzQ1H4dTlUGKKdALzEWemM6mA; expires=Fri, 10-Oct-2025 23:41:11 GMT; Max-Age=7776000; path=/; domain=.facebook.com; secure; httponly
set-cookie: sb=1_jyaEDhyMP_l1pKWxWGVrsp; expires=Sun, 16-Aug-2026 23:41:11 GMT; Max-Age=34560000; path=/; domain=.facebook.com; secure; httponly
reporting-endpoints: coop_report="https://www.facebook.com/browser_reporting/coop/?minimize=0", default="https://www.facebook.com/ajax/browser_error_reports/?device_level=unknown&bsid=752634458050650748&cpp=C3kcv=102469922&st=1752363671427", permissions_policy="https://www.facebook.com/ajax/browser_error_reports/?report-to: {"max_age":2592000,"endpoints":[{"url":"https://www.facebook.com/browser_reporting/coop/?minimize=0"}],"group":"coop_report","include_subdomains":true}, {"max_age":259200,"endpoints":[{"url":"https://www.facebook.com/ajax/browser_error_reports/?device_level=unknown&bsid=7526344658050650748&cpp=C3kcv=102469922&st=1752363671427"}],"max_age":21600,"endpoints":[{"url":"https://www.facebook.com/ajax/browser_error_reports/"}],"group":"permissions_policy"}"
*frame contains 125K
```

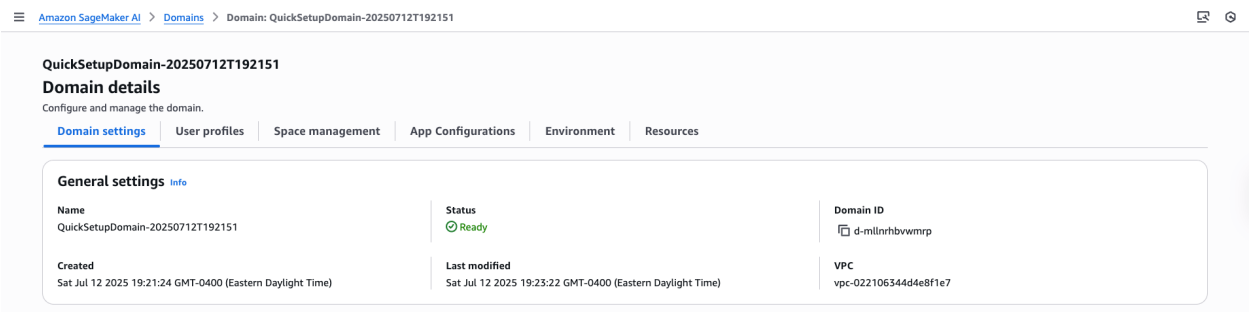
## 2. Sagemaker notebook creation



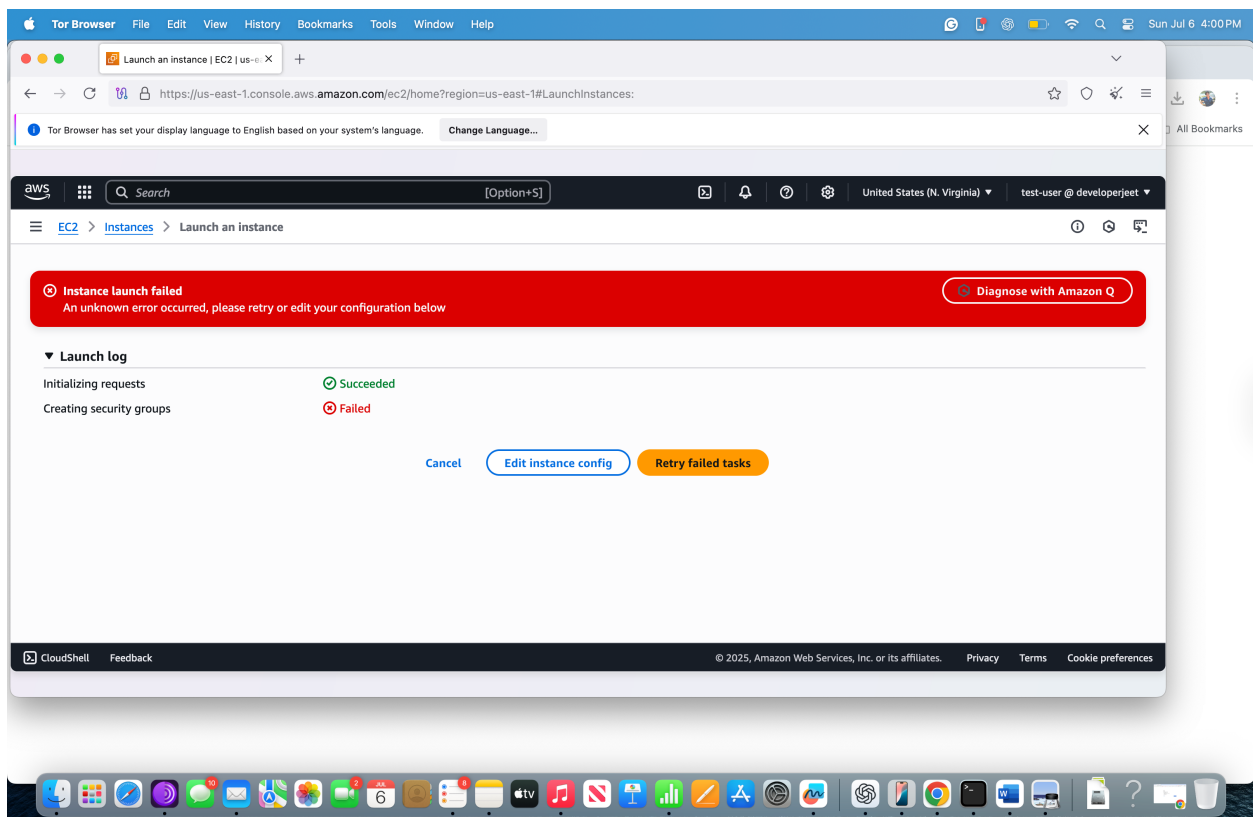
## 3 . Sagemaker Training via jupyter notebook



## 3.Sagemaker deployed



#### 4. Anomaly detection and isolation



## Step 5: Measure the Response Time

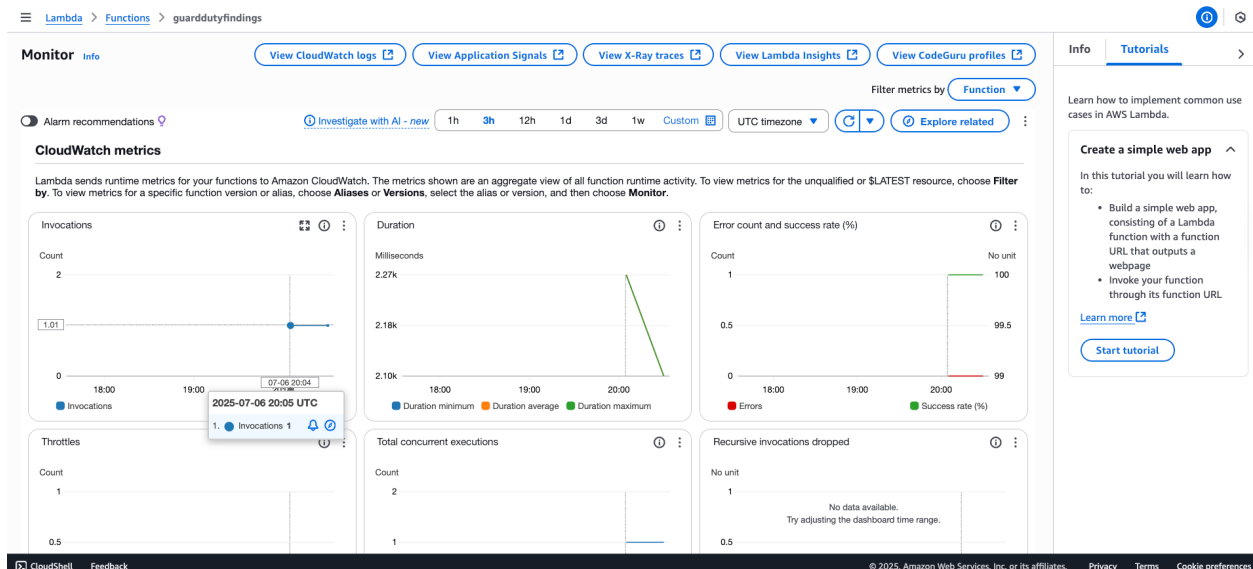
### 1. In CloudTrail, check:

- Time when the user accessed AWS resources

"creationDate": "2025-07-06T20:05:01Z UTC"

- Time when Lambda triggered and blocked the access

2025-07-06T20:05:04Z UTC



Subtract timestamps to calculate response time (goal: under 2 seconds)

2025-07-06T20:05:09.016 - 2025-07-06T20:05:04Z = 3 milliseconds